TRANSLATION OF CERTIFIED DOCUMENT

THIS IS TO CERTIFY THAT ANNEXED US TRUE COPY FROM THE RECORDS OF THIS BUREAU OF THE APPLICATION AS ORIGINALLY FILED WHICH IS IDENTIFIED HEREUNDER.

APPLICATION DATE: 2001/05/25

APPLICATION NUMBER: 090112592 (TITLE: METHOD FOR SECURE ONLINE TRANSACTION)

APPLICANT: Peace Digital Co., LTD.

DIRECTOR OF GENERAL

陳明邦

ISSUE DATE: 2001/06/18

SERIAL NUMBER: 09011008821

中華民國經濟部智慧財產局

INTELLECTUAL PROPERTY OFFICE
MINISTRY OF ECONOMIC AFFAIRS
REPUBLIC OF CHINA

茲證明所附文件，係本局存檔中原申請案的副本，正確無訛，
其申請資料如下 ：

This is to certify that annexed is a true copy from the records of this office of the application as originally filed which is identified hereunder:

申　　請　　日 ： 西元 2001 年 05 月 25 日
Application Date

申　請　案　號 ： 090112592
Application No.

申　　請　　人 ： 平實數位網路股份有限公司
Applicant(s)

局　　長
Director General

陳明邦

發文日期： 西元 2001 年 6 月 18 日
Issue Date

發文字號： 09011008821
Serial No.

申請日期：90、6、25	案號：90112592
類別：	

（以上各欄由本局填註）

發明專利說明書

一、發明名稱	中文	具安全性的網路交易方法
	英文	
二、發明人	姓名（中文）	1. 宋明仲 2. 鄭衍學 3. 涂根皇
	姓名（英文）	1. Ming-Chung Sung 2. Yen-Hsueh Cheng 3. Geng-Hwang Twu
	國籍	1. 中華民國 2. 中華民國 3. 中華民國
	住、居所	1. 台北市大安區正聲里九鄰光復南路308巷39-2號3樓 2. 台中市西屯路三段159-74號9樓之3 3. 屏東縣內埔鄉豐田村興中二巷三號
三、申請人	姓名（名稱）（中文）	1. 平實數位網路股份有限公司
	姓名（名稱）（英文）	1. Peace Digital Marketing Co., LTD.
	國籍	1. 中華民國
	住、居所（事務所）	1. 台北市羅斯福路三段28號4F-1
	代表人姓名（中文）	1. 胡心雄
	代表人姓名（英文）	1. Hsin-Hsiung Hu

四、中文發明摘要　（發明之名稱：具安全性的網路交易方法）

本發明係提供一種網路交易方法，用以提供一使用者藉由一數位媒介進行線上交易。首先，使用者藉由數位媒介於一數位憑證模組中登錄一數位憑證，而後產生一登錄資料，數位憑證模組並會於一預定時間內將登錄資料輸出至一管理模組之認證裝置。接著，使用者藉由數位媒介於一服務提供模組中輸入數位憑證後產生一數位簽章，服務提供模組並會將數位簽章輸出至一管理模組之認證裝置。之後，認證裝置依據一預定的認證程序以確認數位簽章，而後產生一認證識別碼，並將認證識別碼輸出至服務提供模組。之後，服務提供模組藉由認證識別碼以便確認使用者之認證有效狀態，並提供使用者一線上交易服務以產生一相對應之第一交易資料後輸出至一交易帳務模組。之

英文發明摘要　（發明之名稱：）

四、中文發明摘要　（發明之名稱：具安全性的網路交易方法）

後，交易帳務模組在處理第一交易資料後會產生一第二交易資料，並將第二交易資料輸出至管理模組之交易裝置。之後，交易裝置會紀錄下第二交易資料，並將第二交易資料輸出至服務提供模組。最後，服務提供模組會顯示第二交易資料予使用者。其中該數位簽章、該認證識別碼、該第一交易資料以及該第二交易資料於網路線上傳輸過程中，均以該數位憑證為基礎來進行加密保護。

英文發明摘要　（發明之名稱：）

本案已向

國(地區)申請專利	申請日期	案號	主張優先權
無			

有關微生物已寄存於	寄存日期	寄存號碼
無		

五、發明說明 (1)

發明領域

本發明係關於一種網路交易方法，尤指一種結合數位認證之網路交易方法。

發明背景

隨著網際網路的日益盛行，消費者在網路上進行交易的次數也隨之增加。然而，直到今天網路交易的安全性仍然受到相當的質疑。

目前為止，雖然已有許多網路交易方法陸續的被提出，然而其交易的安全性卻都尚嫌不足。習知網路服務提供者(ISP)常利用本身所提供的上網套件為基礎，結合消費網站以提供消費者進行線上交易服務。舉例而言，首先，消費者可以購入該服務提供者一預定面額的上網套件，該上網套件可同時作為上網傳輸費以及線上交易之用。接著，該網路服務提供者便依據消費者的上網時數以及於該消費網站之線上消費金額，進行該上網套件的扣款。最後，當該上網套件之額度用完後，消費者可於線上續購或再買上網套件儲值。

請參閱圖一，圖一為習知網路交易方法10的流程圖。當一消費者於一網路服務提供者購買一預定金額之上網套件後，接著連結至一消費網站上欲進行一消費金額之線上交易時，習知網路交易方法10包含有：

步驟12：於該消費網站中，輸入該上網套件之一預定帳號與密碼，以及將該帳號與密碼傳送至該網路服務者之一電腦系統；

步驟14：於該網路服務者之電腦系統中，根據一預存資料以進行一帳號密碼比對程序，其中該預存資料包含所有上網套件的帳號與密碼；

步驟16：如果帳號與密碼正確，便進行該上網套件之可用餘額R與消費金額C之比較程序；

步驟18：如果該上網套件之可用餘額R大於或等於該消費金額C時，便進行該上網套件之扣款動作，並將交易完成之訊息回傳至該消費網站上；

步驟20：如果該上網套件之可用餘額R小於該消費金額C時，便將交易失敗之訊息回傳至該消費網站上；

步驟22：如果帳戶與密碼不正確，便將交易失敗之訊息回傳至該消費網站上。

然而，利用習知網路交易方法10會有下列缺點：（1）消費者在網路上進行線上交易時，由於帳號與密碼必須在網路上進行傳輸，若遭不當攔截將引發一連串網路交易安全的相關問題。（2）上網套件的帳號與密碼易遭第三者竊取而不當使用，此舉常常造成消費者、網路服務提供者以及消費網站等三方之不必要糾紛。

因此，本發明的主要目的在於提供一種具安全性的網路交易方法，以解決上述問題。

發明概述

本發明在於提供一種應用於一網路交易系統之網路交易方法，用以提供一使用者藉由一數位媒介進行線上交易。首先，使用者藉由數位媒介於一數位憑證模組中登錄

一數位憑證，而後產生一登錄資料，數位憑證模組並會於一預定時間內將登錄資料輸出至一管理模組之認證裝置。接著，使用者藉由數位媒介於一服務提供模組中輸入數位憑證後產生一數位簽章，服務提供模組並會將數位簽章輸出至一管理模組之認證裝置。之後，認證裝置依據一預定認證程序以確認數位簽章，而後產生一認證識別碼，並將認證識別碼輸出至服務提供模組。之後，服務提供模組藉由認證識別碼以便確認使用者之認證有效狀態，並提供使用者一線上交易服務以產生一相對應之第一交易資料後輸出至一交易帳務模組。之後，交易帳務模組在處理第一交易資料後會產生一第二交易資料，並將第二交易資料輸出至管理模組之交易裝置。之後，交易裝置會紀錄下第二交易資料，並將第二交易資料輸出至服務提供模組。最後，服務提供模組會顯示第二交易資料予使用者。

因此，本發明藉由提供一種將數位憑證之認證程序以及線上交易之處理程序分別獨立運作的網路交易方法，其中數位簽章、認證識別碼、第一交易資料以及第二交易資料於網路線上傳輸過程中，均以該數位憑證為基礎來進行加密保護藉以提高網路交易的安全性。

關於本發明之優點與精神可以藉由以下的發明詳述及所附圖式得到進一步的瞭解。

發明之詳細說明

本發明網路交易方法30應用於一網路交易系統32，用以提供一使用者藉由一數位媒介Dm經由一上網裝置34以進

行線上交易。其中，數位媒介Dm可以是一數位交易卡或是一生物辨識裝置，而上網裝置34可以是一個人電腦上網裝置、或是一無線通訊上網裝置、或是一視訊轉換器(Set-top Box)。

請參閱圖二，圖二為應用本發明之網路交易系統32之示意圖。網路交易系統32包含有一數位憑證模組38、一服務提供模組40、一管理模組42以及一交易帳務模組44，其中服務提供模組40可以是一網際網路服務提供者(ISP)或是一網際網路內容提供者(ICP)。管理模組42具有一認證裝置46以及一交易裝置48。認證裝置46通信連接於服務提供模組40以及數位憑證模組38之間，而交易裝置48通信連接於服務提供模組40以及交易帳務模組44之間，其中認證裝置46以及交易裝置48係分別獨立運作於管理模組42之中。

此外，網路交易系統32另包含有一虛擬帳戶模組64，通信連接於交易帳務模組44，用以因應數位媒介Dm以提供一相對應之帳戶資料，其中該帳戶資料包含有一儲值金額。而使用者可以藉由一自動櫃員機(ATM)以進行相關的轉帳程序來更新該帳戶資料之儲值金額。

請參閱圖三，圖三為本發明網路交易方法30之流程圖。本發明網路交易方法30包含有以下步驟：

步驟50：使用者藉由數位媒介Dm經由上網裝置34於數位憑證模組38中登錄一數位憑證Ca，而後產生一登錄資料ID，數位憑證模組38並會於一預定時間內將登錄資料ID輸

出至管理模組42之認證裝置46。其中，登錄資料ID可以包含有數位媒介Dm之已啟動訊息以及一憑證密碼Pw，或者是包含有數位媒介Dm之已啟動訊息、憑證密碼Pw以及使用者之身份證字號與出生年月日等等，而憑證密碼Pw可以由數位憑證模組38所指定或是由使用者自行設定。

步驟52：使用者經由上網裝置34於服務提供模組40中藉由數位媒介Dm輸入數位憑證Ca以及憑證密碼Pw，而後產生一數位簽章Si，服務提供模組40並會將數位簽章Si輸出至管理模組42之認證裝置46。

步驟54：依據一預定認證程序55以確認數位簽章Si，而後產生一認證識別碼Cd。其中，預定認證程序55可以是於認證裝置46中根據登錄資料ID以確認數位簽章Si。

步驟56：服務提供模組40藉由認證識別碼Cd以便確認使用者之認證有效狀態，同時並提供使用者一線上交易服務以產生一相對應之第一交易資料D1後輸出至交易帳務模組44。其中，第一交易資料D1可以包含有該線上交易服務之交易金額、服務項目、交易日期以及廠商代碼等等。

步驟58：交易帳務模組44會處理第一交易資料D1後會產生一第二交易資料D2，並將第二交易資料D2輸出至管理模組42之交易裝置48。第二交易資料D2可能是一包含交易結果之資料或是一無法成交之訊息。

步驟60：交易裝置48會紀錄下第二交易資料D2，並將第二交易資料D2輸出至服務提供模組40。

步驟62：服務提供模組40會顯示第二交易資料D2予使

用者。

其中，本發明網路交易方法30之數位簽章Si、認證識別碼ID、第一交易資料D1以及第二交易資料D2在線上傳輸過程中，均以數位憑證Ca為基礎以1024 bits編碼來進行加密保護。

於本發明之步驟50至步驟56中，使用者首先可以利用具有儲值金額之數位媒介Dm於數位憑證模組38中登錄數位憑證Ca以及憑證密碼Pw。之後，於服務提供模組40中利用數位媒介Dm以輸入數位憑證Ca以及憑證密碼Pw後產生數位簽章Si。之後，數位簽章Si經由管理模組42之認證裝置46的認證後，服務提供模組40才能正式確認使用者之登入狀態而進入交易程序。

於本發明之步驟56至步驟62中，使用者於服務提供模組40中接受一線上交易服務後產生一包含消費金額之第一交易資料D1。接著，交易帳務模組44會根據數位媒介Dm所對應之儲值金額以處理第一交易資料D1後會產生第二交易資料D2。之後，第二交易資料D2會儲存於管理模組42之交易裝置48中。最後，服務提供模組40會將交易結果顯示於使用者之上網裝置34上。

因此，本發明網路交易方法30藉由提供一種具有獨立運作之憑證認證程序(步驟50至步驟56)以及交易程序(步驟56至步驟62)，其中由於數位簽章Si、認證識別碼ID、第一交易資料D1以及第二交易資料D2在線上傳輸過程中，均以數位憑證Ca為基礎以1024 bits編碼來進行加密保

護，因此網路交易安全性的問題將會被大幅改善。另外，本發明網路交易方法30中交易帳務模組44除了即時將第二交易資料D2輸出至交易裝置48外，還可以定期分批次將第二交易資料D2輸出至交易裝置48，因此交易裝置48可以定期比對第二交易資料D2中的交易結果資料，藉以防止交易結果資料被惡意竄改之虞。

於本發明另一實施例中，網路交易系統32亦可以包含有複數個管理模組42，每一管理模組42係用來管理一特定族群之對應數位媒介Dm'。使用者可藉由對應數位媒介Dm'於數位憑證模組38中登錄一對應數位憑證Ca'，而後產生一對應登錄資料ID'，數位憑證模組38會將對應登錄資料ID'輸出至其所對應的管理模組42之認證裝置46。而對應登錄資料ID'會分別被儲存於數位憑證模組38以及其所對應的管理模組42之認證裝置46中，因此，一方面可以節省資料傳輸的時間，一方面亦可以擴大整個交易服務的範圍，讓應用本發明網路交易方法30的網站能有較好的服務品質與反應速度。

請參閱圖四，圖四為圖三所示預定認證程序57另一實施例之流程圖。於本發明網路交易方法30中，步驟54之預定認證程序57亦可以包含有以下子步驟：

步驟54a：檢測數位憑證Dm與管理模組42是否具有對應關係。

步驟54b：若數位憑證Dm與管理模組42具有對應關係，則藉由儲存於對應認證裝置46中的對應登錄資料ID'

以確認數位簽章Si，並因而產生認證識別碼Cd，以及將認證識別碼Cd輸出至服務提供模組40。

步驟54c：若數位憑證Dm與管理模組42無對應關係，則認證裝置46會將數位簽章Si輸出至數位憑證模組38，並藉由儲存於數位憑證模組38中的對應登錄資料ID'以確認數位簽章Si，並因而產生認證識別碼Cd，以及將認證識別碼Cd經由認證裝置46而輸出至服務提供模組40。

於本發明之步驟50至步驟56中，使用者首先可以利用具有儲值金額之對應數位媒介Dm'於數位憑證模組38中登錄對應數位憑證Ca'以及對應憑證密碼Pw'。之後，於服務提供模組40中利用對應數位媒介Dm'以輸入對應數位憑證Ca'以及對應憑證密碼Pw'後產生數位簽章Si。之後，服務提供模組40便會將數位簽章Si輸出至其所對應管理模組42之認證裝置46。之後，數位簽章Si便可以藉由其所對應管理模組42之認證裝置46的認證後，服務提供模組40才能正式確認使用者之登入狀態而進入交易程序。此外，若服務提供模組40因某些因素而未將數位簽章Si傳送到其所對應之管理模組42之認證裝置46，數位簽章Si亦可經由無對應關係的管理模組42之認證裝置46，藉由儲存於數位憑證模組38中的對應登錄資料ID'以確認數位簽章Si。

相較於習知網路交易方法10，由於本發明網路交易方法30提供獨立運作的憑證認證程序(步驟50至步驟56)以及交易程序(步驟56至步驟62)，其中由於數位簽章Si、認證識別碼ID、第一交易資料D1以及第二交易資料D2在線上傳

輸過程中，均以數位憑證Ca為基礎以1024 bits編碼來進行加密保護，比起SSL來說，保護程度更高，因此網路交易安全性的問題將會被大幅改善。另外，本發明網路交易方法30中交易帳務模組44除了即時將第二交易資料D2輸出至交易裝置48外，還可以定期分批次將第二交易資料D2輸出至交易裝置48，因此交易裝置48可以定期比對第二交易資料D2中的交易結果資料，藉以防止交易結果資料被惡意竄改之虞。

藉由以上較佳具體實施例之詳述，係希望能更加清楚描述本發明之特徵與精神，而並非以上述所揭露的較佳具體實施例來對本發明之範疇加以限制。相反地，其目的是希望能涵蓋各種改變及具相等性的安排於本發明所欲申請之專利範圍的範疇內。

圖式簡單說明

圖一為習知網路交易方法之流程圖。

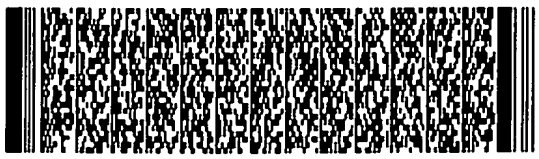
圖二為應用本發明之網路交易系統之示意圖。

圖三為本發明網路交易方法之流程圖。

圖四為圖三所示預定認證程序另一實施例之流程圖。

圖式之符號說明

30 網路交易方法	32 網路交易系統
34 上網裝置	38 數位憑證模組
40 服務提供模組	42 管理模組
44 交易帳務模組	46 認證裝置
48 交易裝置	64 虛擬帳戶模組



六、申請專利範圍

1、一種應用於一網路交易系統之網路交易方法，用以提供一使用者藉由一數位媒介進行線上交易，該網路交易系統包含有一數位憑證模組、至少一服務提供模組、至少一管理模組以及一交易帳務模組，每一管理模組分別具有一認證裝置以及一交易裝置，該認證裝置通信連接於該服務提供模組以及該數位憑證模組之間，該交易裝置通信連接於該服務提供模組以及該交易帳務模組之間，該網路交易方法包含有：

該使用者藉由該數位媒介於該數位憑證模組中登錄一數位憑證，而後產生一登錄資料，該數位憑證模組並會於一預定時間內將該登錄資料輸出至該管理模組之認證裝置；

該使用者藉由該數位媒介於該服務提供模組中輸入該數位憑證而後產生一數位簽章，該服務提供模組並會將該數位簽章輸出至該管理模組之認證裝置；

依據一預定認證程序以確認該數位簽章，而後產生一認證識別碼；

該服務提供模組藉由該認證識別碼以便確認該使用者之認證有效狀態，並提供該使用者一線上交易服務以產生一相對應之第一交易資料後輸出至該交易帳務模組；

該交易帳務模組在處理該第一交易資料後會產生一第二交易資料，並將該第二交易資料輸出至該管理模組之交易裝置；

該交易裝置會紀錄下該第二交易資料，並將該第二交易資料輸出至該服務提供模組；以及

六、申請專利範圍

該服務提供模組會顯示該第二交易資料予該使用者；

其中該數位簽章、該認證識別碼、該第一交易資料以及該第二交易資料於網路線上傳輸過程中，均以該數位憑證為基礎來進行加密保護。

2、如申請專利範圍第1項之方法，其中該認證裝置以及該交易裝置係分別獨立運作於該管理模組之中。

3、如申請專利範圍第2項之方法，其中每一管理模組係因應於一對應的數位媒介，該使用者可藉由該對應的數位媒介於該數位憑證模組中登錄一對應的數位憑證，而後產生一對應的登錄資料，該對應的登錄資料則會分別被儲存於該數位憑證模組以及其所對應的管理模組之認證裝置中。

4、如申請專利範圍第3項之方法，其中該認證裝置之預定認證程序包含有下列步驟：

(1)檢測該數位憑證與該管理模組是否具有對應關係；以及

(2)若該數位憑證與該管理模組具有對應關係，則藉由儲存於該對應認證裝置中的對應登錄資料以確認數位簽章，並因而產生該認證識別碼，以及將該認證識別碼輸出至該服務提供模組。

5、如申請專利範圍第4項之方法，其中於步驟(2)中若該數位憑證與該管理模組無對應關係，則該認證裝置會將該數位簽章輸出至該數位憑證模組，並藉由儲存於該數位憑證模組中的對應登錄資料以確認該數位簽章，並因而產生該認證識別碼，以及將該認證識別碼經由該認證裝置而輸

出至該服務提供模組。

6、如申請專利範圍第2項之方法，其中該預定認證程序係為該認證裝置藉由該登錄資料以確認該數位簽章，以及將該認證識別碼輸出至該服務提供模組。

7、如申請專利範圍第1項之方法，其中該網路交易系統另包含有一虛擬帳戶模組，通信連接於該交易帳務模組，用以提供一帳戶資料，該虛擬帳戶模組並可提供該使用者藉由一預定方式來更新該帳戶資料。

8、如申請專利範圍第7項之方法，其中該預定方式為經由一自動櫃員機(ATM)以進行相關的轉帳程序。

9、如申請專利範圍第1項之方法，其中該數位媒介可以是一數位交易卡。

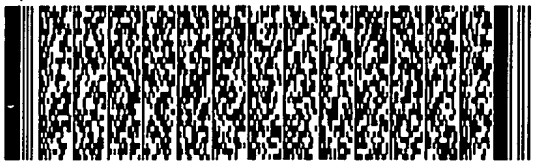
10、如申請專利範圍第1項之方法，其中該數位媒介可以是一生物辨識裝置。

申請案件名稱:具安全性的網路交易方法

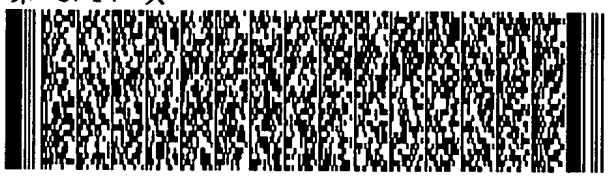
第 1/17 頁

第 2/17 頁

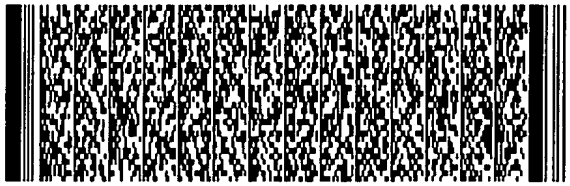
第 3/17 頁



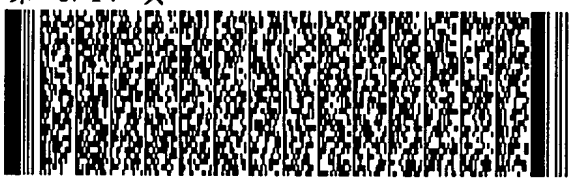
第 5/17 頁



第 5/17 頁

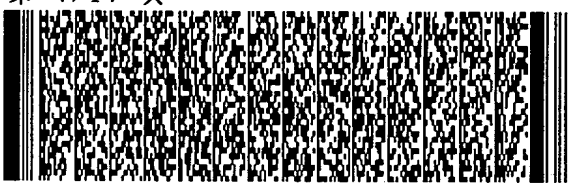


第 6/17 頁

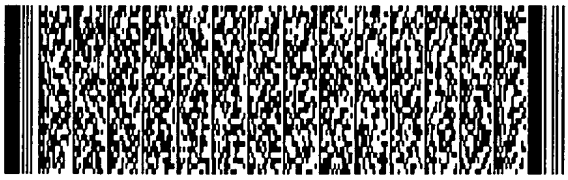


第 6/17 頁

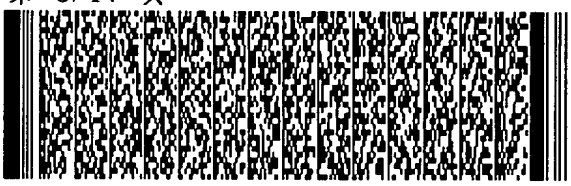
第 7/17 頁



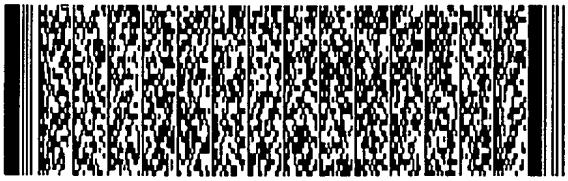
第 7/17 頁



第 8/17 頁



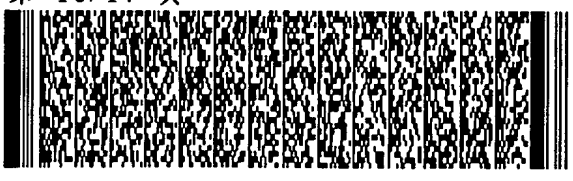
第 8/17 頁



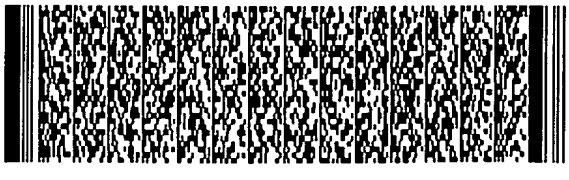
第 9/17 頁

第 9/17 頁

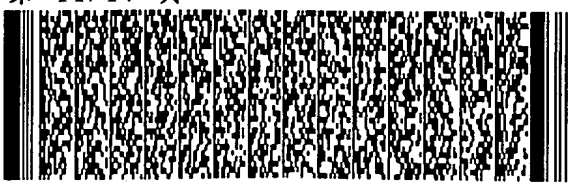
第 10/17 頁



第 10/17 頁



第 11/17 頁



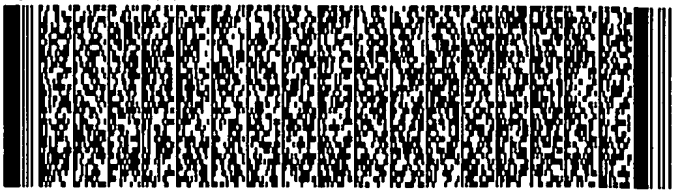
申請案件名稱:具安全性的網路交易方法

第 11/17 頁

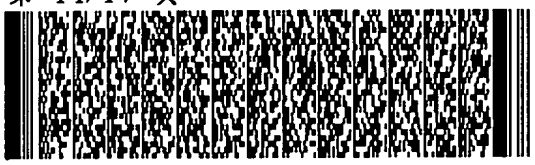
第 12/17 頁

第 12/17 頁

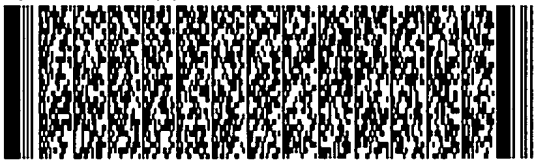
第 13/17 頁



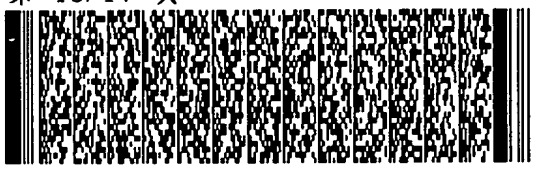
第 14/17 頁



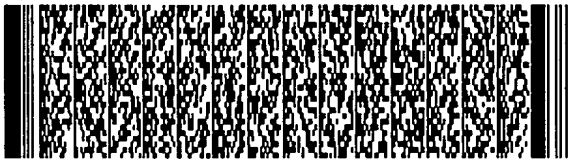
第 15/17 頁



第 15/17 頁



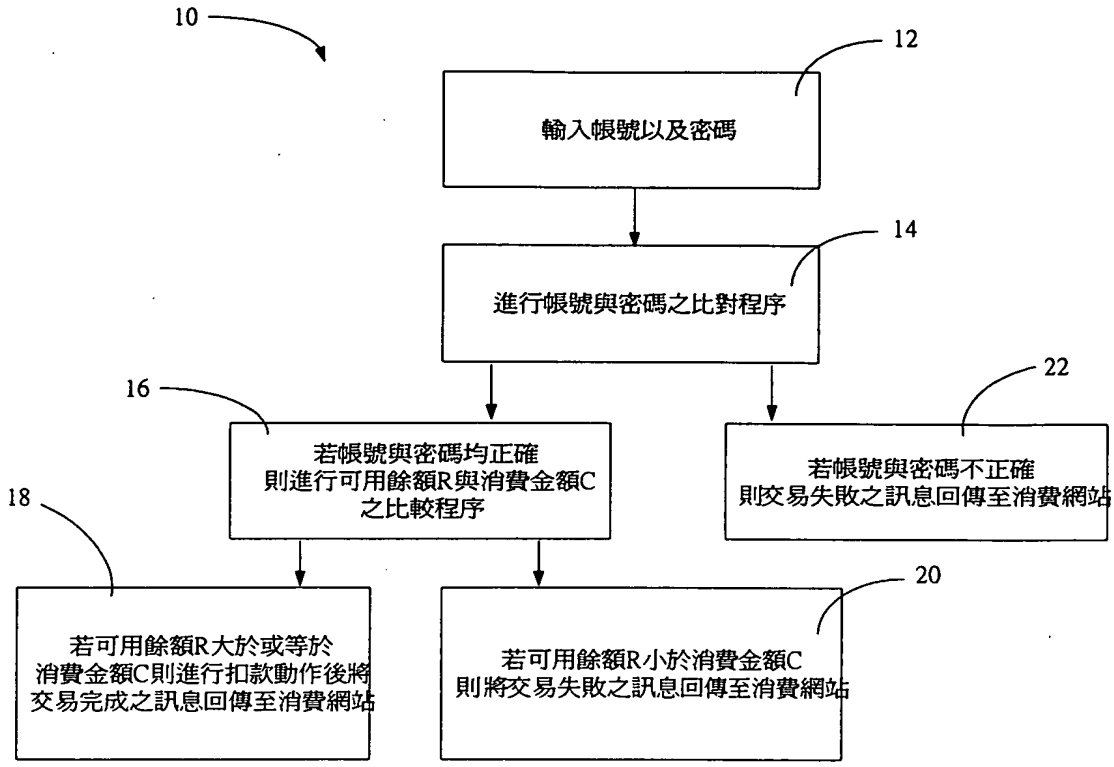
第 16/17 頁



第 16/17 頁

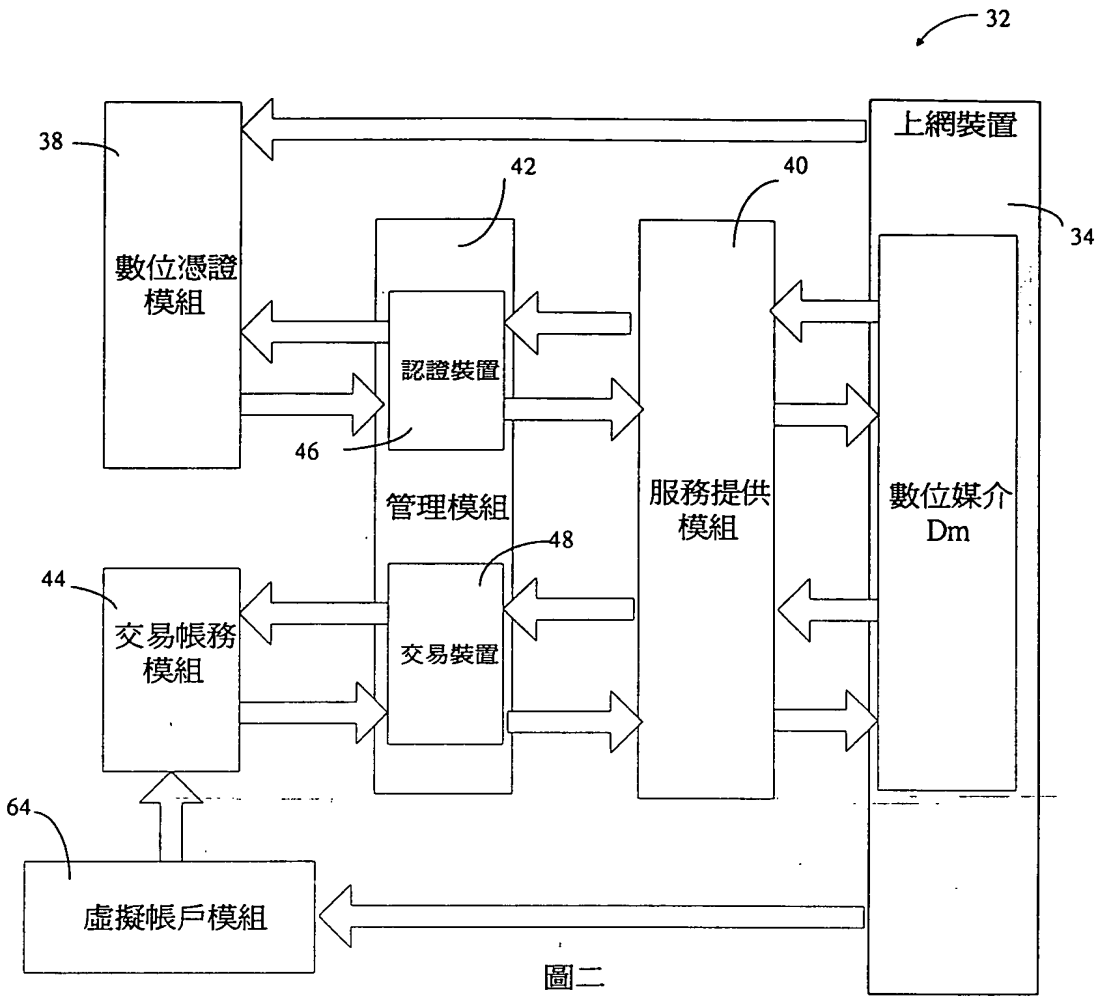
第 17/17 頁

圖式


10
12
輸入帳號以及密碼
14
進行帳號與密碼之比對程序
16
若帳號與密碼均正確
則進行可用餘額R與消費金額C
之比較程序
22
若帳號與密碼不正確
則交易失敗之訊息回傳至消費網站
18
若可用餘額R大於或等於
消費金額C則進行扣款動作後將
交易完成之訊息回傳至消費網站
20
若可用餘額R小於消費金額C
則將交易失敗之訊息回傳至消費網站

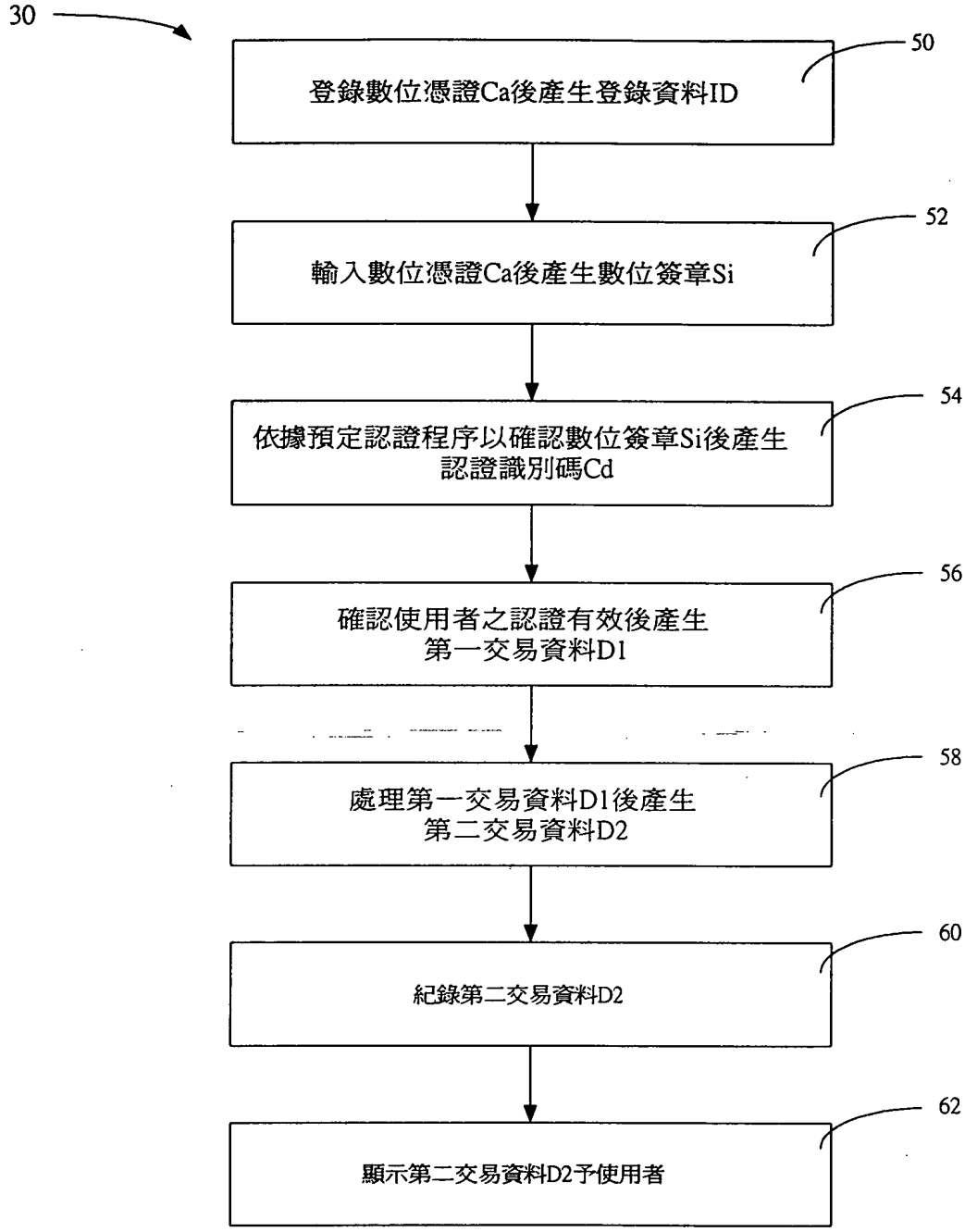
圖一 習知技術

圖式


32
上網裝置
38
42
40
34
數位憑證
模組
認證裝置
46
管理模組
服務提供
模組
數位媒介
Dm
48
44
交易帳務
模組
交易裝置
64
虛擬帳戶模組

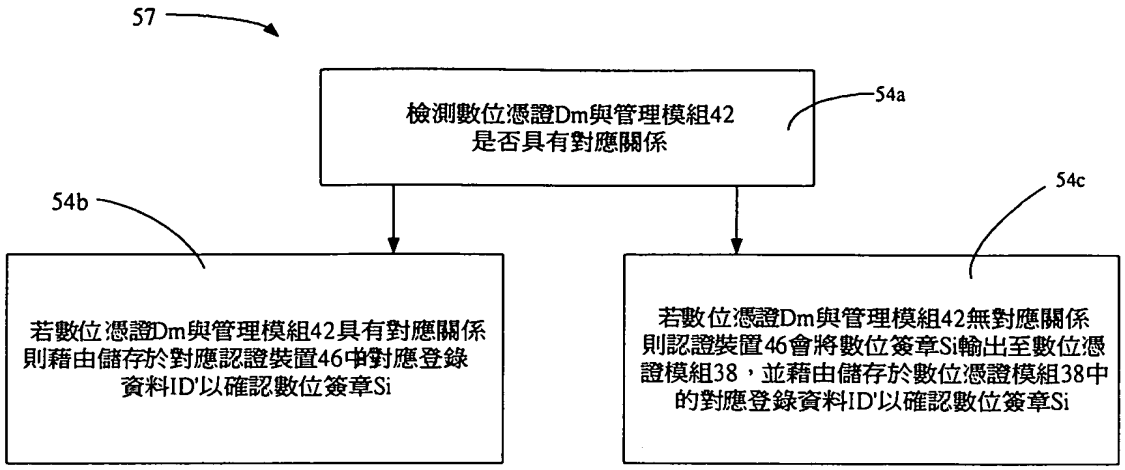
圖二

圖式


30
登錄數位憑證Ca後產生登錄資料ID
50
輸入數位憑證Ca後產生數位簽章Si
52
依據預定認證程序以確認數位簽章Si後產生認證識別碼Cd
54
確認使用者之認證有效後產生第一交易資料D1
56
處理第一交易資料D1後產生第二交易資料D2
58
紀錄第二交易資料D2
60
顯示第二交易資料D2予使用者
62

圖三

圖式


57
檢測數位憑證Dm與管理模組42
是否具有對應關係
54a
54b
54c
若數位憑證Dm與管理模組42具有對應關係
則藉由儲存於對應認證裝置46中對應登錄
資料ID'以確認數位簽章Si
若數位憑證Dm與管理模組42無對應關係
則認證裝置46會將數位簽章Si輸出至數位憑
證模組38，並藉由儲存於數位憑證模組38中
的對應登錄資料ID'以確認數位簽章Si

圖四